

# THE GRAPHIC NATURE OF CYCLIC SUPERCHARACTERS

STEPHAN RAMON GARCIA AND BOB LUTZ

**ABSTRACT.** We investigate supercharacters of finite cyclic groups arising from actions of cyclic automorphism groups. The visually arresting graphs of so-called *cyclic supercharacters* indicate an underlying geometry that can be explicitly formulated in some cases. We present a gallery of notable and recurrent qualitative features, proving statements that quantify them.

## 1. INTRODUCTION

In the following, we assume that the reader has a working knowledge of the character theory of finite groups [3, 4]. P. Diaconis and I. M. Isaacs recently introduced the theory of *supercharacters*, which generalizes classical character theory.

**Definition** (Diaconis-Isaacs [2]). Let  $G$  be a finite group with identity 0,  $\mathcal{K}$  a partition of  $G$ , and  $\mathcal{X}$  a partition of the set  $\text{Irr}(G)$  of irreducible characters of  $G$ . The ordered pair  $(\mathcal{X}, \mathcal{K})$  is a *supercharacter theory* for  $G$  if

- (i)  $\{0\} \in \mathcal{K}$ ,
- (ii)  $|\mathcal{X}| = |\mathcal{K}|$ ,
- (iii) For each  $X \in \mathcal{X}$ , the character

$$\sigma_X = \sum_{\chi \in X} \chi(0)\chi \quad (1)$$

is constant on each  $K \in \mathcal{K}$ .

The characters  $\sigma_X$  are called *supercharacters* of  $G$ . The elements of  $\mathcal{K}$  are called *superclasses*.

In what follows, we consider supercharacters of  $\mathbb{Z}/n\mathbb{Z}$  arising from the action of a cyclic subgroup  $A$  of  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ . Since each automorphism of  $\mathbb{Z}/n\mathbb{Z}$  has the form  $x \mapsto ux$  for some unit  $u$ , we consider  $A$  to be a cyclic subgroup of the unit group  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Let  $\mathcal{K}$  denote the set of all orbits of  $\mathbb{Z}/n\mathbb{Z}$  under the action of  $A$ . Clearly, the orbit of 0 is  $\{0\}$ , so that (i) holds.

For all real numbers  $\theta$ , let  $e(\theta) = \exp(i2\pi\theta)$ . As is well known, the irreducible characters of  $\mathbb{Z}/n\mathbb{Z}$  are given by  $\chi_x(y) = e(\frac{xy}{n})$ , where  $x$  belongs to  $\mathbb{Z}/n\mathbb{Z}$ . We consider the action of  $A$  on  $\text{Irr}(\mathbb{Z}/n\mathbb{Z})$  given by  $a \cdot \chi_x = \chi_{a^{-1}x}$  for all  $a$  in  $A$  and  $x$  in  $\mathbb{Z}/n\mathbb{Z}$ , so that

$$(a \cdot \chi_x)(a \cdot y) = e\left(\frac{a^{-1}xay}{n}\right) = e\left(\frac{xy}{n}\right) = \chi_x(y).$$

It follows from a lemma of R. Brauer [3, Cor. 6.33] that the action of  $A$  partitions  $\mathbb{Z}/n\mathbb{Z}$  and  $\text{Irr}(\mathbb{Z}/n\mathbb{Z})$  into an equal number of orbits. Thus, letting  $\mathcal{X}$  be the set of all orbits of  $\text{Irr}(\mathbb{Z}/n\mathbb{Z})$  under the action of  $A$  gives  $|\mathcal{X}| = |\mathcal{K}|$ , so that (ii) holds.

---

Partially supported by National Science Foundation Grant DMS-1001614.

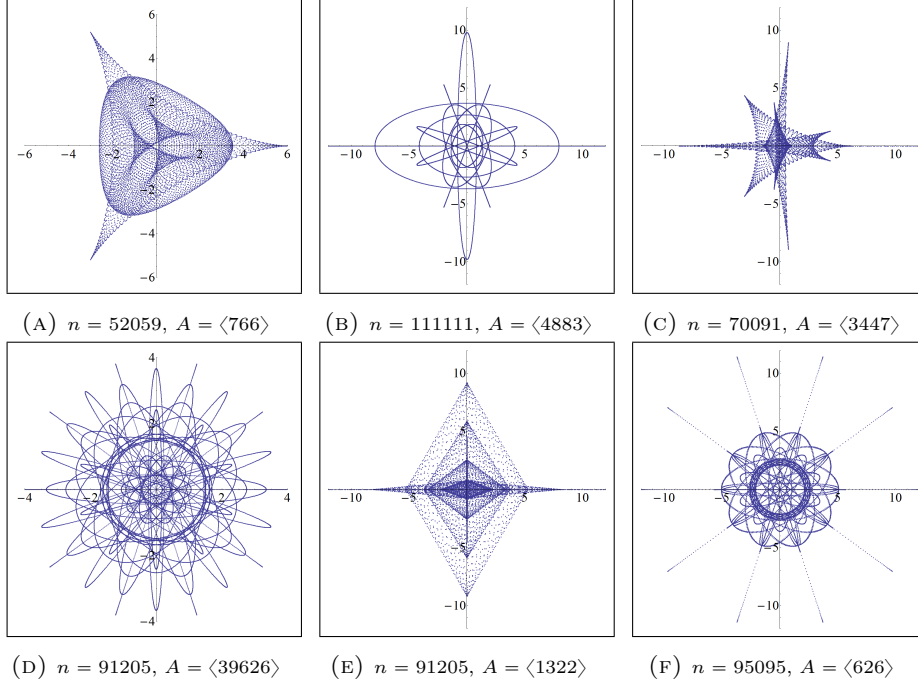


FIGURE 1. Cyclic supercharacters of  $\mathbb{Z}/n\mathbb{Z}$  arise from actions of cyclic automorphism groups. Each subfigure is the graph of a cyclic supercharacter  $\sigma_X$ , where  $X$  is the orbit of  $r = 1$  under the action of  $A \leq (\mathbb{Z}/n\mathbb{Z})^\times$  on  $\mathbb{Z}/n\mathbb{Z}$  by multiplication.

For all parts  $X$  in  $\mathcal{X}$ , we identify each character  $\chi_x$  in  $X$  with the corresponding residue  $x$  modulo  $n$ , so that  $X$  is stable under the action  $x \mapsto ax$  of  $A$ . With this convention, the functions  $\sigma_X$  defined in (2) are given by

$$\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{n}\right). \quad (2)$$

If  $y' = ay$  for some  $a$  in  $A$ , then for all  $X$  in  $\mathcal{X}$ , we have

$$\sigma_X(y') = \sum_{x \in X} e\left(\frac{xay}{n}\right) = \sum_{x \in X} e\left(\frac{axy}{n}\right) = \sum_{x' \in X} e\left(\frac{x'y}{n}\right) = \sigma_X(y).$$

Each  $\sigma_X$  is therefore constant on each  $K$  in  $\mathcal{K}$ , so that (iii) holds. Hence  $(\mathcal{X}, \mathcal{K})$  is a supercharacter theory for  $\mathbb{Z}/n\mathbb{Z}$ , and the  $\sigma_X$  as given above, are the corresponding supercharacters.

We call supercharacters arising in this way *cyclic*. The graphs of cyclic supercharacters are visually striking and considerably diverse, as illustrated in Figures 1 and 2. Moreover, cyclic supercharacters are a kind of generalization of quadratic Gauss sums; we develop this connection in Section 4.2.

## 2. BASIC CYCLIC SUPERCHARACTER GEOMETRY

Following the introduction, we identify each  $X$  in  $\mathcal{X}$  with the orbit  $Ar$  of an element  $r$  of  $\mathbb{Z}/n\mathbb{Z}$  under the action of a cyclic subgroup  $A$  of  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

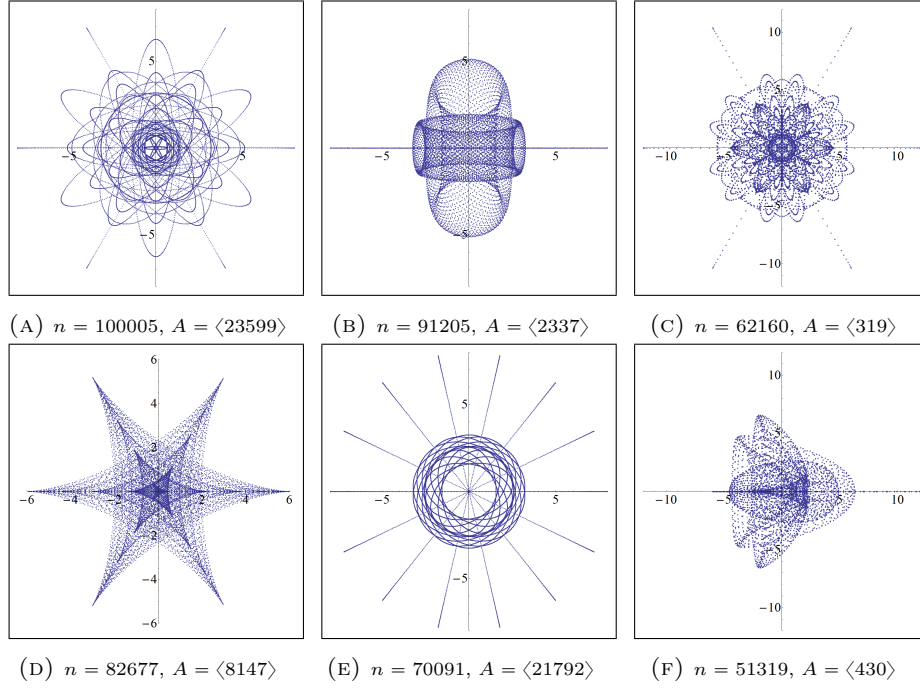


FIGURE 2. More graphs of cyclic supercharacters  $\sigma_X$ , where each set  $X$  is the orbit of  $r = 1$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$

by multiplication. For every positive divisor  $d$  of  $n$ , let  $\psi_d$  be the ring homomorphism that maps each element of  $\mathbb{Z}/n\mathbb{Z}$  to its residue modulo  $d$ . If  $A = \langle u \rangle$  acts on  $\mathbb{Z}/n\mathbb{Z}$  by multiplication, then  $\psi_d(A) = \langle \psi_d(u) \rangle$  is a unit modulo  $d$  and so acts on  $\mathbb{Z}/d\mathbb{Z}$ , again by multiplication. As a consequence of the following result, we observe all possible graphical behaviors of cyclic supercharacters by restricting our attention to the case  $r = 1$ .

**Theorem 2.1.** *Let  $r$  belong to  $\mathbb{Z}/n\mathbb{Z}$ , and suppose that  $(r, n) = \frac{n}{d}$  for some positive divisor  $d$  of  $n$ , so that  $\xi = \frac{rd}{n}$  is a unit modulo  $n$ . Further let  $X_g^n$  be the orbit of  $g$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$  for  $g = r, \xi, \frac{n}{d}$ , and let  $X_1^d$  be the orbit of 1 under the action of  $\psi_d(A)$  on  $\mathbb{Z}/d\mathbb{Z}$ .*

- (i) *The images of  $\sigma_{X_r^n}$ ,  $\sigma_{X_{n/d}^n}$ , and  $\sigma_{X_1^d}$  are equal.*
- (ii) *The image in (i), after scaling by  $\frac{|A|}{|\psi_d(A)|}$ , is a subset of the image of  $\sigma_{X_\xi^n}$ .*

*Proof.* For each orbit  $X_g^m$ , let  $A_g^m$  be a subset of  $A$  such that  $|A_g^m| = |X_g^m|$  and  $X_g^m = \{ag : a \in A_g^m\}$ . Since  $\frac{a\xi n}{d} \equiv \frac{a'\xi n}{d} \pmod{n}$  iff  $\frac{an}{d} \equiv \frac{a'n}{d} \pmod{n}$ , we may assume that  $A_r^n = A_{n/d}^n$ . For any  $y$  in  $\mathbb{Z}/d\mathbb{Z}$ , letting  $y' = \xi^{-1}y$  gives

$$\sigma_{X_r^n}(y') = \sum_{x \in X_r^n} e\left(\frac{xy'}{n}\right) = \sum_{a \in A_r^n} e\left(\frac{a\xi y'}{d}\right) = \sum_{a \in A_{n/d}^n} e\left(\frac{ay}{d}\right) = \sigma_{X_{n/d}^n}(y),$$

so the image of  $\sigma_{X_r^n}$  contains that of  $\sigma_{X_{n/d}^n}$ . Letting  $y' = \xi y$  instead gives

$$\sigma_{X_{n/d}^n}(y') = \sum_{a \in A_{n/d}^n} e\left(\frac{ay'}{n}\right) = \sum_{a \in A_r^n} e\left(\frac{a\xi y}{n}\right) = \sigma_{X_r^n}(y),$$

proving the reverse containment. Since  $\frac{an}{d} \equiv \frac{a'n}{d} \pmod{n}$  iff  $a \cdot 1 \equiv a' \cdot 1 \pmod{d}$ , we may assume that  $A_{n/d}^n = A_1^d$ . We have

$$\sigma_{X_{n/d}^n}(y) = \sum_{a \in A_{n/d}^n} e\left(\frac{ay}{d}\right) = \sum_{a \in A_1^d} e\left(\frac{ay}{d}\right) = (\sigma_{X_1^d} \circ \psi_d)(y),$$

since the function  $e$  is periodic with period 1. Hence the images of  $\sigma_{X_{n/d}^n}$  and  $\sigma_{X_1^d}$  are equal, proving (i). Since  $ar \equiv a'r \pmod{n}$  iff  $a \equiv a' \pmod{d}$ , we may assume that  $A_r^n = \psi_d(A_\xi^n)$ . For any  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ , letting  $y' = \frac{yn}{d}$  gives

$$\sigma_{X_\xi^n}(y') = \sum_{a \in A_\xi^n} e\left(\frac{ay'}{d}\right) = \frac{|A_\xi^n|}{|\psi_d(A_\xi^n)|} \sum_{a \in \psi_d(A_\xi^n)} e\left(\frac{ay}{d}\right) = \frac{|A|}{|\psi_d(A)|} \sigma_{X_r^n}(y),$$

proving that the image of  $\sigma_{X_\xi^n}$  contains that of  $\frac{|A|}{|\psi_d(A)|} \sigma_{X_r^n}$ .  $\square$

**Proposition 2.2.** *The maximum modulus of  $\sigma_{X_r^n}$  is  $|\psi_d(A)|$ .*

*Proof.* It follows from (2) that

$$|\sigma_{X_\xi^n}(y)| \leq \sigma_{X_\xi^n}(0) = |X_\xi^n| = |A|$$

for all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ . Theorem 2.1(ii) now gives

$$\max_{y \in \mathbb{Z}/n\mathbb{Z}} |\sigma_{X_r^n}(y)| = \frac{|\psi_d(A)|}{|A|} \max_{y \in \mathbb{Z}/n\mathbb{Z}} |\sigma_{X_\xi^n}(y)| = |\psi_d(A)|,$$

as desired.  $\square$

**Example 2.3.** Let  $n = 62160 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 37$ . Each graph in Figure 3 displays the image of a different cyclic supercharacter  $\sigma_X$ , where  $X$  is the orbit of  $\frac{n}{d}$  under the action of  $\langle 319 \rangle$  on  $\mathbb{Z}/n\mathbb{Z}$  for some given positive divisor  $d$  of  $n$ . By Theorem 2.1(i), each is equivalent to the image of  $\sigma_{X_1^d}$  where  $X_1^d$  is the orbit of 1 under the action of  $\psi_d(\langle 319 \rangle) = \langle \psi_d(319) \rangle$  on  $\mathbb{Z}/d\mathbb{Z}$ . By Theorem 2.1(ii), each is a scaled subset of the graph in Figure 3(F).

### 3. SYMMETRIES

We provide sufficient conditions for axial and rotational symmetries in the images of cyclic supercharacters. We say that  $\sigma_X$  has *k-fold dihedral symmetry* if its image is invariant under the natural action of the dihedral group of order  $2k$ . In other words,  $\sigma_X$  has *k-fold dihedral symmetry* if its image is invariant under complex conjugation and rotation by  $2\pi/k$  about the origin.

**Proposition 3.1.** *Suppose that  $\sigma_X$  is a cyclic supercharacter of  $\mathbb{Z}/n\mathbb{Z}$ .*

- (i) *The supercharacter  $\sigma_X$  has 1-fold dihedral symmetry (i.e., its image is symmetric about the real axis).*
- (ii) *If  $X$  is the orbit of  $r$  where  $(r, n) = \frac{n}{d}$  for some even divisor  $d$  of  $n$ , then  $\sigma_X$  has 2-fold dihedral symmetry.*

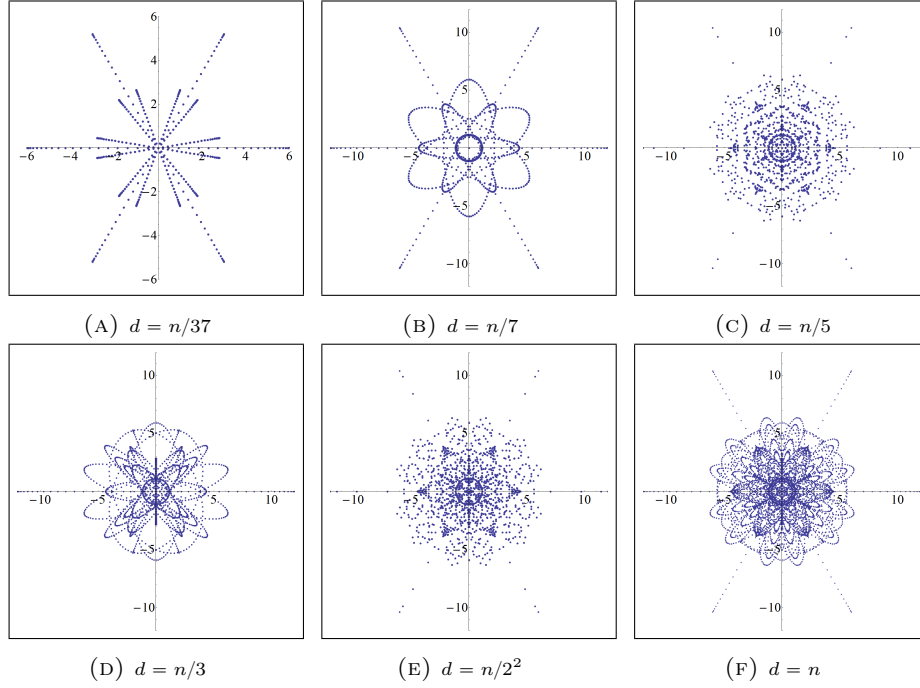


FIGURE 3. Fixing  $n = 62160$ , each subfigure is the graph of  $\sigma_X$ , where  $X$  is the orbit of  $\frac{n}{d}$  under the action of  $\langle \psi_d(319) \rangle$  on  $\mathbb{Z}/n\mathbb{Z}$ , considering  $\psi_d(319)$  as an element of  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Each image is scaled subset of the one in Figure 3(F).

*Proof of (i).* For all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ , the image of  $\sigma_X$  contains both  $\sigma_X(y)$  and its complex conjugate  $\sigma_X(y) = \sigma_X(-y)$ .  $\square$

We defer the proof of Proposition 3.1(ii) to the end of the section. Figure 4 illustrates asymmetries of certain  $\sigma_X$  about the imaginary axis in cases where  $X$  is the orbit of  $r$  with  $(r, n) = \frac{n}{d}$  for some odd divisor  $d$  of  $n$ . Because rotational and axial symmetries are invariant under scaling, we examine only the situation  $r = 1$  in light of Theorem 2.1.

**Lemma 3.2.** *Suppose that  $k$  is a positive divisor of  $n$ , and that  $(\xi, k) = 1$ . If for each  $y$  in  $\mathbb{Z}/n\mathbb{Z}$  there exists a solution  $y'$  in  $\mathbb{Z}/n\mathbb{Z}$  of the congruence*

$$xy' \equiv xy + \frac{\xi n}{k} \pmod{n}, \quad (3)$$

*then  $\sigma_X$  has  $k$ -fold dihedral symmetry.*

*Proof.* If the hypothesis of the Lemma holds, then since the function  $e$  is periodic with period 1, we have

$$\sum_{x \in X} e\left(\frac{xy'}{n}\right) = \sum_{x \in X} e\left(\frac{xy + \xi n/k}{n}\right) = e\left(\frac{\xi}{k}\right) \sum_{x \in X} e\left(\frac{xy}{n}\right),$$

i.e., the graph of  $\sigma_X$  is invariant under counterclockwise rotation by  $2\pi\xi/k$  about the origin. If  $m$  is the multiplicative inverse of  $\xi$  modulo  $k$ , then the graph is also

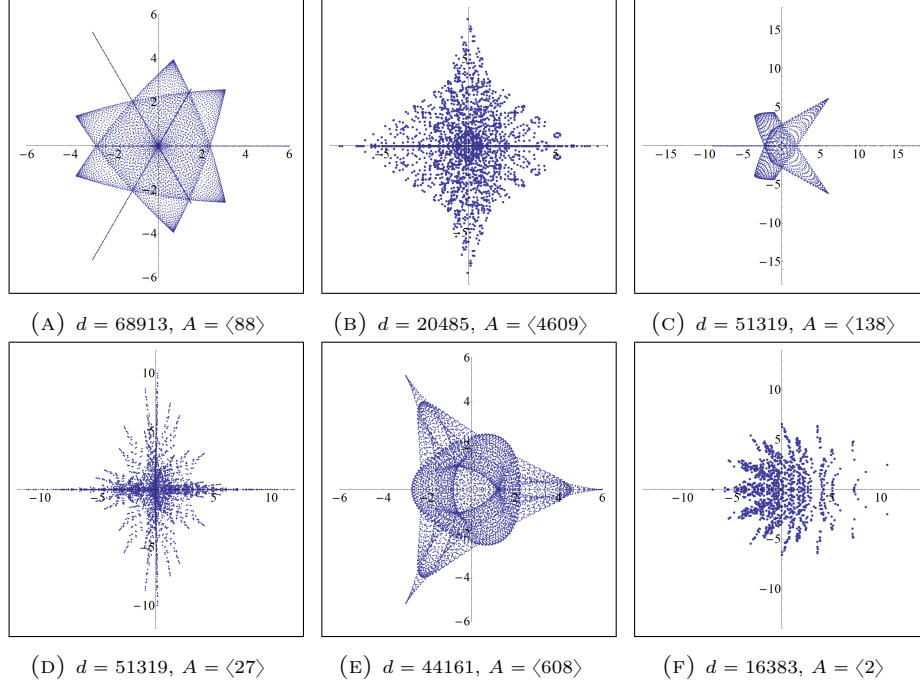


FIGURE 4. Odd values of  $d$  can produce asymmetric images. Each subfigure is the graph of  $\sigma_X$ , where  $X$  is the orbit of  $r = 1$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ , so that  $d = n$  in all cases (a close examination reveals that image (E) does *not* have 3-fold symmetry).

invariant under counterclockwise rotation by  $m \cdot 2\pi\xi/k = 2\pi/k$ . That the symmetry is dihedral now follows from Proposition 3.1(i).  $\square$

**Theorem 3.3.** *If  $X$  is the orbit of  $r$  under the action of  $A = \langle u \rangle$  on  $\mathbb{Z}/n\mathbb{Z}$ , where  $(r, n) = \frac{n}{d}$  for some positive divisor  $d$  of  $n$ , then  $\sigma_X$  has  $(u - 1, d)$ -fold dihedral symmetry.*

*Proof.* If  $k = (u - 1, d)$ , then the generator  $u$ , and hence every element of  $A$ , has the form  $jk + 1$ . If  $(r, n) = \frac{n}{d}$ , then  $r = \frac{\xi n}{d}$  where  $(\xi, n) = 1$ . Each  $x$  in  $X$  therefore has the form  $\frac{\xi n}{d}(jk + 1)$ . If  $y' = y + \frac{d}{k}$ , then  $y' - y - \frac{d}{k} \equiv 0 \pmod{n}$ , in which case

$$\frac{\xi n}{d}(jk + 1) \left( y' - y - \frac{d}{k} \right) \equiv 0 \pmod{n}.$$

It follows that

$$(jk + 1) \left[ \frac{\xi n}{d}(y' - y) - \frac{\xi n}{k} \right] \equiv 0 \pmod{n},$$

whence

$$\begin{aligned} \frac{\xi n}{d}(jk + 1)y' &\equiv \frac{\xi n}{d}(jk + 1)y + \frac{\xi n}{k}(jk + 1) \pmod{n} \\ &\equiv \frac{\xi n}{d}(jk + 1)y + \frac{\xi n}{k} \pmod{n}, \end{aligned}$$

but this is (3).  $\square$

**Example 3.4.** For all  $m = 1, 2, 3, 4, 6, 8, 12$ , let  $X_m$  denote the orbit of 1 under the action of  $\langle 4609 \rangle$  on  $\mathbb{Z}/(20485m)\mathbb{Z}$ . Consider the cyclic supercharacter  $\sigma_{X_1}$ , whose graph appears in Figure 4(B). We have  $(20485, 4608) = (5 \cdot 17 \cdot 241, 2^9 \cdot 3^2) = 1$ , so Theorem 3.3 guarantees that  $\sigma_{X_1}$  has 1-fold dihedral symmetry. In particular, it is visibly apparent that  $\sigma_X$  has only the trivial rotational symmetry. Figures 5(A) to 5(F) display the graphs of  $\sigma_{X_m}$  in the cases  $m \neq 1$ . For each such  $m$ , the graph of  $\sigma_{X_m}$  contains a scaled copy of  $\sigma_{X_1}$  by Theorem 2.1 and has  $m$ -fold dihedral symmetry by Theorem 3.3, since  $(20485m, 4608) = (20485, 4608)(m, 4608) = 1 \cdot m$ . It is apparent from the associated figures that  $m$  is maximal in each case, in the sense that  $\sigma_{X_m}$  having  $k$ -fold dihedral symmetry implies  $k \leq m$ .

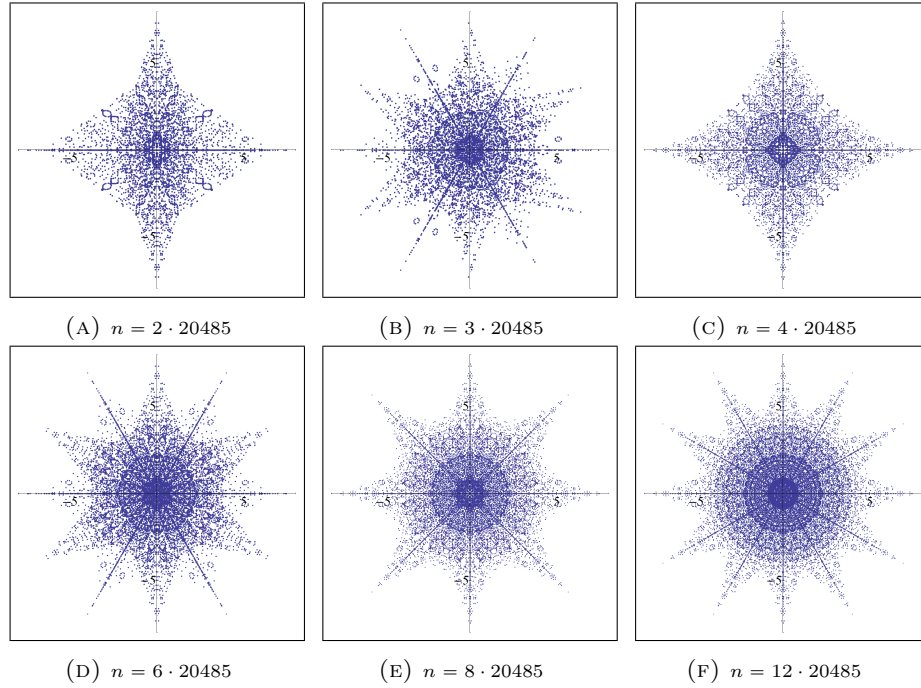


FIGURE 5. Each subfigure is the graph of  $\sigma_X$  where  $X$  is the orbit of 1 under the action of  $\langle 4609 \rangle$  on  $\mathbb{Z}/n\mathbb{Z}$ . By taking multiples of  $n$ , we produce dihedrally symmetric images containing the one in Figure 4(B).

*Proof of Proposition 3.1(ii).* Suppose that  $\sigma_X$  is a cyclic supercharacter of  $\mathbb{Z}/n\mathbb{Z}$ , and that  $X$  is the orbit of  $r$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$  where  $(r, n) = \frac{n}{d}$  for some positive divisor  $d$  of  $n$ . If  $A = \langle u \rangle$  for some unit  $u > 1$  modulo  $n$ , then  $u$  is necessarily odd, whence  $u - 1$  is even. Therefore  $2|(u - 1, d)$ , so the result follows from Theorem 3.3.  $\square$

#### 4. SHAPES OF CYCLIC SUPERCHARACTERS

**4.1. Real and imaginary supercharacters.** The images of many cyclic supercharacters are subsets of the real axis. Many more are subsets of the union of the

real and imaginary axes. In this section, we establish sufficient conditions for each situation to occur and provide explicit evaluations in certain cases.

**Example 4.1.** Suppose that  $A = \langle -1 \rangle$ . If  $X = Ar$  where  $r = \frac{n}{2}$ , then  $X = \{r\}$ , in which case  $\sigma_X(y) = e(\frac{ry}{n})$  for all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ . If  $r \neq \frac{n}{2}$ , then  $X = \{-r, r\}$ , so

$$\sigma_X(y) = e\left(\frac{ry}{n}\right) + e\left(-\frac{ry}{n}\right) = e\left(\frac{ry}{n}\right) + \overline{e\left(\frac{ry}{n}\right)} = 2 \cos \frac{2\pi ry}{n},$$

for all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ . Figure 6(A) illustrates this situation, in which the distribution of points in the image of  $\sigma_X$  is visibly sinusoidal.

**Proposition 4.2.** Suppose that  $X$  is the orbit of  $r$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ . If  $A$  contains  $-1$ , then the graph of  $\sigma_X$  is a subset of the real axis.

*Proof.* By Theorem 2.1(i), it suffices to consider  $r = 1$ , in which case  $X = A$ . Since  $X$  is a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$  containing  $-1$ , it is closed under negation. In particular,  $x \mapsto -x$  is a permutation of  $X$ , since otherwise  $x \equiv -x \pmod{n}$  contradicts that  $x$  is a unit. Hence

$$\sigma_X(y) = \sum_{x \in X} e\left(\frac{xy}{n}\right) = \sum_{x \in X} e\left(-\frac{xy}{n}\right) = \overline{\sigma_X(y)},$$

for all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ . □

**Example 4.3.** Let  $X$  be the orbit of 3 under the action of  $\langle 164 \rangle$  on  $\mathbb{Z}/855\mathbb{Z}$ . Since  $164^3 \equiv -1 \pmod{n}$ , the proof of Proposition 4.2 implies that  $X$  is closed under negation. Indeed,  $X = \{\pm 3, \pm 318, \pm 363\}$ . Figure 7(c) confirms that  $\sigma_X$  is real.

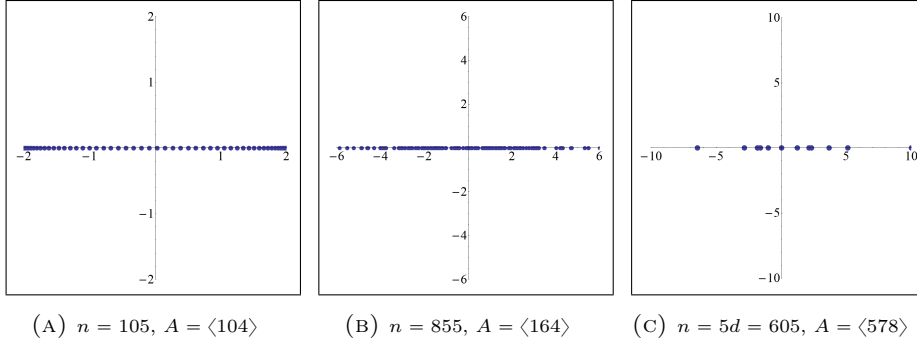


FIGURE 6. Each subfigure is the graph of  $\sigma_X$ , where  $X$  is the orbit of 1 under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ . Each  $\sigma_X$  is real-valued, since each  $A$  contains  $-1$ .

We turn our attention to  $\sigma_X$  whose values on  $\mathbb{Z}/n\mathbb{Z}$ , if not real, are purely imaginary. Let  $k$  be a positive divisor of  $n$ , and suppose that

$$A = \left\langle \frac{j_0 n}{k} - 1 \right\rangle, \quad \text{for some } 1 \leq j_0 < k. \quad (4)$$

In this situation, we have

$$\left( \frac{j_0 n}{k} - 1 \right)^m \equiv (-1)^m \pmod{\frac{n}{k}},$$



so that every element of  $A$  has either the form  $\frac{jn}{k} + 1$  or  $\frac{jn}{k} - 1$ , where  $0 \leq j < k$ . In this situation, we write

$$A = \left\{ \frac{jn}{k} + 1 : j \in J_+ \right\} \cup \left\{ \frac{jn}{k} - 1 : j \in J_- \right\} \quad (5)$$

for some subsets  $J_+$  and  $J_-$  of  $\{0, 1, \dots, k-1\}$ . Several remarks are in order; first, the condition (5) is vacuous if  $k = n$ . However, if  $k < n$  and  $j_0 > 1$  (i.e., if  $A$  is nontrivial), then it follows that  $(-1)^{|A|} \equiv 1 \pmod{\frac{n}{k}}$ , whence  $|A|$  is even. In particular, this implies  $|J_+| = |J_-|$ . The subsets  $J_+$  and  $J_-$  are not necessarily disjoint; if, e.g.,  $A = \langle -1 \rangle = \{-1, 1\}$ , then (5) holds where  $k = 1$  and  $J_+ = J_- = \{0\}$ . In general,  $J_+$  must contain 0, since  $A$  must contain 1.

**Proposition 4.4.** *Suppose that  $X$  is the orbit of  $r$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ , and that (5) holds, where  $k$  is even and  $J_- = \frac{k}{2} - J_+$ .*

- (i) *If  $r$  is even, then the image of  $\sigma_X$  is a subset of the real axis.*
- (ii) *If  $r$  is odd, then the image of  $\sigma_X$  is a subset of the real and imaginary axes. In particular,  $\sigma_X(y)$  is real if  $y$  is even and purely imaginary if  $y$  is odd.*

**Example 4.5.** In the case of Figure 7(B), we have  $n = 912$ ,  $r = 1$ ,  $k = 38$ ,  $j_0 = 3$ ,

$$J_+ = \{0, 2, 12, 16, 20, 22, 24, 26, 32\}, \quad \text{and} \quad J_- = \{3, 7, 17, 19, 25, 31, 33, 35, 37\},$$

so the hypotheses of Proposition 4.4(ii) hold.

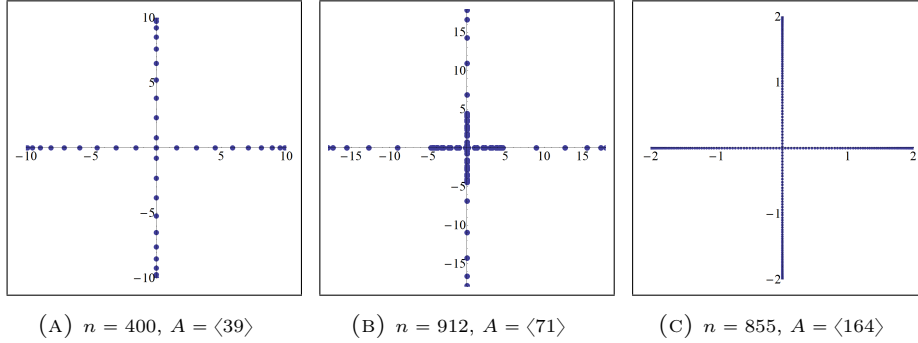


FIGURE 7. Some cyclic supercharacters have values that are either real or purely imaginary. Each subfigure is the graph of  $\sigma_X$  where  $X$  is the orbit of 1 under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ .

*Proof of Proposition 4.4.* Each  $x$  in  $X$  has the form  $(\frac{jn}{k} + 1)r$  or

$$\left[ \frac{(\frac{k}{2} - j)n}{k} + 1 \right] r = \left( \frac{n}{2} - \frac{jn}{k} + 1 \right) r.$$

If  $y = 2m$  for some integer  $m$ , then for every summand  $e(\frac{xy}{n})$  in the expression (2) for  $\sigma_X(y)$  having the form

$$e\left(\frac{2m(\frac{jn}{k} + 1)r}{n}\right) = e\left(\frac{2mjr}{k} + \frac{2m}{d}\right), \quad (6)$$

there is one of the form

$$\begin{aligned} e\left(\frac{2m\left(\frac{n}{2} - \frac{jn}{k} + 1\right)r}{n}\right) &= e\left(mr - \frac{2mjr}{k} - \frac{2m}{d}\right) \\ &= e\left(-\frac{2mjr}{k} - \frac{2m}{d}\right), \end{aligned}$$

which is the complex conjugate of (6). From this we deduce that  $\sigma_X(y)$  is real whenever  $y$  is even. Suppose instead that  $y = 2m + 1$ . For every  $e(\frac{xy}{n})$  of the form

$$e\left(\frac{(2m+1)\left(\frac{jn}{k} + 1\right)r}{n}\right) = e\left(\frac{(2m+1)jr}{k} + \frac{2m+1}{d}\right), \quad (7)$$

there is one of the form

$$\begin{aligned} e\left(\frac{(2m+1)\left(\frac{n}{2} - \frac{jn}{k} + 1\right)r}{n}\right) &= e\left(mr + \frac{r}{2} - \frac{(2m+1)jr}{k} - \frac{2m+1}{d}\right) \\ &= e\left(\frac{r}{2} - \frac{(2m+1)j}{k} - \frac{2m+1}{d}\right). \end{aligned} \quad (8)$$

If  $r$  is odd, then (8) is (7) reflected across the imaginary axis, in which case  $\sigma_X(y)$  is purely imaginary. If  $r$  is even, (8) is the complex conjugate of (7), in which case  $\sigma_X(y)$  is real.  $\square$

An explicit evaluation of  $\sigma_X$  is available if  $J_+ \cup J_- = \{0, 1, \dots, k-1\}$ . The following result treats this situation, an instance of which is illustrated by Figure 7(A).

**Proposition 4.6.** *Suppose that  $k > 2$  is even, and that (5) holds where  $J_+$  is the set of all even residues modulo  $k$  and  $J_-$  is the set of all odd residues. If  $X$  is the orbit of a unit  $r$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ , then*

$$\sigma_X(y) = \begin{cases} k \cos \frac{2\pi ry}{n} & \text{if } k|y, \\ ik \sin \frac{2\pi ry}{n} & \text{if } y \equiv \frac{k}{2} \pmod{k}, \\ 0 & \text{else.} \end{cases}$$

*Proof.* We have  $(\frac{2\ell n}{k} + 1)r \equiv (\frac{2\ell' n}{k} + 1)r \pmod{n}$  iff  $\ell \equiv \ell' \pmod{\frac{k}{2}}$ , so letting  $J = \{0, 1, \dots, \frac{k}{2} - 1\}$  gives

$$\left\{\left(\frac{jn}{k} + 1\right)r : j \in J_+\right\} = \left\{\left(\frac{2jn}{k} + 1\right)r : j \in J\right\}.$$

Since  $(\frac{2\ell n}{k} + 1)r \equiv (\frac{2\ell' n}{k} + 1)r \pmod{n}$  iff  $[\frac{(2\ell+1)n}{k} - 1]r \equiv [\frac{(2\ell'+1)n}{k} - 1]r \pmod{n}$ , we also have

$$\left\{\left(\frac{jn}{k} - 1\right)r : j \in J_-\right\} = \left\{\left[\frac{(2j+1)n}{k} - 1\right]r : j \in J\right\}.$$

We now compute

$$\begin{aligned} \sigma_X(y) &= \left[\sum_{j \in J'_+} e\left(\frac{(\frac{jn}{k} + 1)ry}{n}\right)\right] + \left[\sum_{j \in J'_-} e\left(\frac{(\frac{jn}{k} - 1)ry}{n}\right)\right] \\ &= \left[e\left(\frac{ry}{n}\right) \sum_{j \in J} e\left(\frac{2jry}{k}\right)\right] + \left[\overline{e\left(\frac{ry}{n}\right)} \sum_{j \in J} e\left(\frac{(2j+1)ry}{k}\right)\right] \end{aligned}$$

$$= \left[ e\left(\frac{ry}{n}\right) + \overline{e\left(\frac{ry}{n} - \frac{ry}{k}\right)} \right] \sum_{j=0}^{k/2-1} e\left(\frac{2jry}{k}\right)$$

If  $k$  divides  $y$ , then

$$\sigma_X(y) = \frac{k}{2} \left[ e\left(\frac{y}{d}\right) + \overline{e\left(\frac{y}{n}\right)} \right] = k \cos \frac{2\pi ry}{n}.$$

If  $k$  divides  $2y$  but not  $y$ , then since the function  $e$  is periodic with period 1,

$$\sigma_X(y) = \frac{k}{2} \left[ e\left(\frac{ry}{n}\right) + \overline{e\left(\frac{ry}{n} - \frac{1}{2}\right)} \right] = ik \sin \frac{2\pi ry}{n}.$$

Suppose that  $k$  does not divide  $2ry$ . The set  $\{e(\frac{jry}{k/2}) : 0 \leq j \leq \frac{k}{2} - 1\}$  is the set of primitive roots of unity of degree  $\frac{k}{2} > 1$  and hence has zero sum.  $\square$

**4.2. Circles and Ellipses.** The graphs of cyclic supercharacters contain instances of familiar geometric shapes. The following results and examples address the types of numerical relationships that produce such objects. We first address the appearance of concentric circles about the origin.

Suppose that  $k$  is a positive divisor of  $n$ . If  $A = \langle \frac{j_0 n}{k} + 1 \rangle$  for some  $1 \leq j_0 < k$ , then an analog of (5) holds where  $J_-$  is empty. That is, there exists a subset  $J$  of  $\{0, 1, \dots, k-1\}$  such that  $|J| = |A|$  and

$$A = \left\{ \frac{jn}{k} + 1 : j \in J \right\}. \quad (9)$$

**Proposition 4.7.** *Suppose that (9) holds, and let  $X$  be the orbit of  $r$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ , where  $(r, n) = \frac{n}{d}$ .*

- (i) *If  $k|(j-j')ry$  for all  $j, j' \in J$ , then  $|\sigma_X(y)| = |\psi_d(A)|$  (i.e., is maximal).*
- (ii) *If  $J = \{0, 1, \dots, k-1\}$ , then*

$$\sigma_X(y) = \begin{cases} \frac{k}{(r,k)} e\left(\frac{ry}{n}\right) & \text{if } k|ry, \\ 0 & \text{else.} \end{cases}$$

- (iii) *If  $|J| = k-1$ , then  $|\sigma_X(y)| = |\psi_d(A)|$  if  $k|ry$  and otherwise  $|\sigma_X(y)| = 1$ .*

*Proof.* We have

$$\sigma_X(y) = \sum_{j \in J} e\left(\frac{\left(\frac{jn}{k} + 1\right)ry}{n}\right) = e\left(\frac{ry}{n}\right) \sum_{j \in J} e\left(\frac{jry}{k}\right). \quad (10)$$

Therefore  $|\sigma_X(y)| = |J| = |X|$  if  $jry \equiv j'ry \pmod{k}$  for all  $j$  and  $j'$  in  $J$ . This congruence is equivalent to  $k|(j-j')ry$ , proving (i). We now prove (ii). If  $J = \{0, 1, \dots, k-1\}$ , then the set  $\{e(\frac{xy}{n}) : x \in X\}$  is  $(ry, k)$  copies of a rotation of the set of  $\frac{k}{(ry, k)}$ -primitive roots of unity. Therefore if  $k|ry$ , then the degree of the roots is 1, so it follows from (10) that

$$\sigma_X(y) = |X| e\left(\frac{ry}{n}\right) = \frac{k}{(r, k)} e\left(\frac{ry}{n}\right).$$

Otherwise, the degree is at least two, so  $\sigma_X(y) = 0$ .

We now prove (iii). If  $|J| = k - 1$ , then the set  $\{e(\frac{xy}{n}) : x \in X\}$  is  $(ry, k)$  copies of a rotation of the set of  $\frac{k}{(ry, k)}$ -primitive roots of unity, where one copy is missing a single root. Thus if  $k|ry$ , then  $|\sigma_X(y)| = |X|$ , and otherwise  $|\sigma_X(y)| = 1$ .  $\square$

**Example 4.8.** If  $n = d = 525$  and  $A = \langle 176 \rangle$ , then the elements of  $X = \{r, 176r\}$  are distinct, so the hypotheses of Proposition 4.7 hold for  $k = 3$  and  $J = \{0, 1\}$ . Since  $|X| = k - 1$ , we may apply (iii) from the preceding. If  $y$  belongs to  $\mathbb{Z}/n\mathbb{Z}$ , then either  $y$  and  $k$  are coprime, in which case  $|\sigma_X(y)| = 1$ , or else  $k$  divides  $y$ , in which case  $|\sigma_X(y)| = |X| = 2$ . These deductions are illustrated in Figure 8(A), where each point of the graph lies on a circle of radius 1 or 2 centered at the origin.

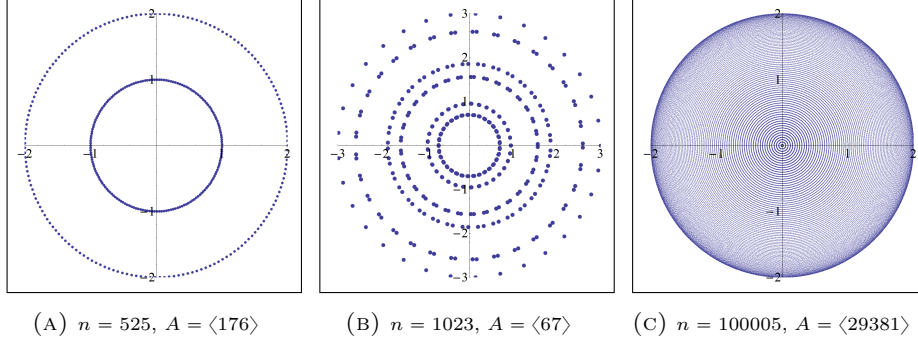


FIGURE 8. The graphs of some cyclic supercharacters resemble concentric circles about the origin. Each subfigure is the graph of  $\sigma_X$ , where  $X$  is the orbit of  $r = 1$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ .

Ellipses also appear frequently in the graphs of cyclic supercharacters, often in great multiplicity and rotated about the origin. We now examine single ellipses whose major axes lie along the imaginary axis.

**Definition.** Suppose that  $m$  and  $k$  are integers with  $k > 0$ . The *quadratic Gauss sum*  $g(m; p)$  over  $\mathbb{Z}/k\mathbb{Z}$  is given by

$$g(m; k) = \sum_{\ell=0}^{k-1} e\left(\frac{m\ell^2}{k}\right). \quad (11)$$

We let  $\left(\frac{m}{p}\right)$  denote the Legendre symbol of  $m$  and  $p$ , and we let

$$Q_p = \left\{ m \in \mathbb{Z}/p\mathbb{Z} : \left(\frac{m}{p}\right) = 1 \right\}$$

be the set of distinct nonzero quadratic residues modulo  $p$ .

**Lemma 4.9** (Berndt [1, Theorem 1.5.2]). *If  $p \equiv 1 \pmod{4}$  is prime and  $(m, p) = 1$ , then*

$$g(m; k) = \left(\frac{m}{k}\right) \sqrt{k}.$$

**Theorem 4.10.** Suppose that  $p|n$  and  $p \equiv 1 \pmod{4}$  is prime. If (5) holds where

$$J_+ = a \cdot Q_p + b \quad \text{and} \quad J_- = c \cdot Q_p - b \quad (12)$$

for integers  $a, b, c$  coprime to  $p$  with  $\left(\frac{a}{p}\right) = -\left(\frac{c}{p}\right)$ , then

$$\sigma_X(y) = \begin{cases} (p-1) \cos \frac{2\pi y}{n} & \text{if } p|y, \\ -\cos \frac{2\pi(bn+py)y}{pn} \pm i\left(\frac{y}{p}\right) \sqrt{p} \sin \frac{2\pi(bn+py)y}{pn} & \text{else,} \end{cases}$$

where the sign depends on  $\left(\frac{a}{p}\right)$ . In particular,  $\sigma_X(y)$  belongs to the real interval  $[1-p, p-1]$  if  $p|y$ , and otherwise belongs to the ellipse  $\{\alpha + i\beta \in \mathbb{C} : \alpha^2 + \beta^2/p = 1\}$ .

**Example 4.11.** Let  $n = d = 1088 = 4^3 \cdot 17$  and consider the orbit  $X$  of  $r = 1$  under the action of  $A = \langle 63 \rangle = \langle \frac{n}{17} - 1 \rangle$  on  $\mathbb{Z}/n\mathbb{Z}$ . In this situation, illustrated by Figure 9(A), (5) holds with  $J_+ = \{0, 4\} = 2 \cdot Q_5 + 2$  and  $J_- = \{2, 4\} = Q_{17} + 3$ . Figure 9(B) illustrates the situation  $J_+ = Q_{13} + 3$  and  $J_- = 2 \cdot Q_{13} - 3$ , while Figure 9(C) illustrates  $J_+ = Q_5 + 1$  and  $J_- = 2 \cdot Q_2 - 1$ . The remainder of Figure 9 demonstrates the effect of using Theorems 2.1, 3.3 and 4.10 to produce supercharacters whose images feature ellipses.

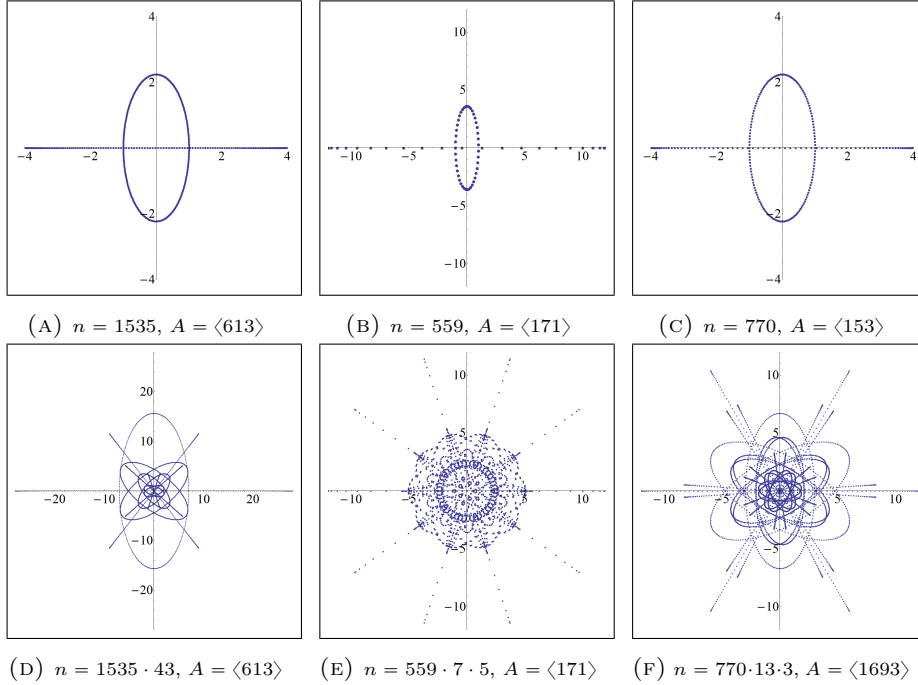


FIGURE 9. Theorems 2.1, 3.3 and 4.10 can be used to produce visually striking images from supercharacters whose graphs contain single ellipses. Each subfigure is the graph of  $\sigma_X$ , where  $X$  is the orbit of 1 under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ .

*Proof of Theorem 4.10.* For all  $y$  in  $\mathbb{Z}/n\mathbb{Z}$ , we have

$$\begin{aligned}
\sigma_X(y) &= \sum_{x \in A} e\left(\frac{xy}{n}\right) \\
&= \sum_{j \in J_+} e\left(\frac{\left(\frac{jn}{p} + 1\right)y}{n}\right) + \sum_{j \in J_-} e\left(\frac{\left(\frac{jn}{p} - 1\right)y}{n}\right) \\
&= \sum_{q \in Q_p} e\left(\frac{(aq + b)y}{p} + \frac{y}{n}\right) + \sum_{q \in Q_p} e\left(\frac{(cq - b)y}{p} - \frac{y}{n}\right) \\
&= \left[ e\left(\frac{by}{p} + \frac{y}{n}\right) \sum_{q \in Q_p} e\left(\frac{aqy}{p}\right) \right] + \left[ e\left(-\frac{by}{p} - \frac{y}{n}\right) \sum_{q \in Q_p} e\left(\frac{cqy}{p}\right) \right] \\
&= \left[ e(\theta_y) \sum_{\ell=1}^{(p-1)/2} e\left(\frac{a\ell^2 y}{p}\right) \right] + \left[ \overline{e(\theta_y)} \sum_{\ell=1}^{(p-1)/2} e\left(\frac{c\ell^2 y}{p}\right) \right],
\end{aligned}$$

where  $\theta_y = \frac{(bn+p)y}{pn}$ . If  $p|y$ , then  $e(\theta_y) = e\left(\frac{y}{n}\right)$  and  $e\left(\frac{a\ell^2 y}{p}\right) = e\left(\frac{c\ell^2 y}{p}\right) = 1$ , so

$$\sigma_X(y) = \frac{(p-1)}{2} \left[ e\left(\frac{y}{n}\right) + \overline{e\left(\frac{y}{n}\right)} \right] = (p-1) \cos \frac{2\pi y}{n}.$$

If not, then  $(p, y) = 1$ , so

$$\begin{aligned}
\sigma_X(y) &= \frac{e(\theta_y)[g(ay; p) - 1] + \overline{e(\theta_y)}[g(cy; p) - 1]}{2} \\
&= \frac{e(\theta_y)g(ay; p) + \overline{e(\theta_y)}g(cy; p)}{2} - \cos 2\pi\theta_y \\
&= \frac{\sqrt{p}}{2} \left[ \left(\frac{ay}{p}\right) e(\theta_y) + \left(\frac{cy}{p}\right) \overline{e(\theta_y)} \right] - \cos 2\pi\theta_y \tag{13} \\
&= \pm \left(\frac{y}{p}\right) \frac{\sqrt{p}}{2} \left[ e(\theta_y) - \overline{e(\theta_y)} \right] - \cos 2\pi\theta_y \\
&= \pm i \left(\frac{y}{p}\right) \sqrt{p} \sin 2\pi\theta_y - \cos 2\pi\theta_y,
\end{aligned}$$

where (13) follows from Lemma 4.9.  $\square$

## 5. OPEN QUESTIONS

Our work suggests several directions of further research in the geometry of supercharacters of  $\mathbb{Z}/n\mathbb{Z}$  arising from the actions of automorphism groups. The following questions in particular remain open.

**Question 5.1.** Suppose that (4) holds. Are there sufficient conditions that can be imposed on  $j_0$  in order to guarantee that  $J_+$  and  $J_-$  satisfy the hypotheses of Propositions 4.4 or 4.6, or of Theorem 4.10?

**Question 5.2.** In considering some of the more visually captivating examples of images of cyclic supercharacters, we have observed the existence of other cyclic supercharacters whose images are geometrically similar, but which feature boundaries that are visibly more rounded. Several examples of such images and their “looped” counterparts appear in Figure 10. Can the relationships between such

supercharacters be quantified? If so, do these relationships carry a group-theoretic significance?

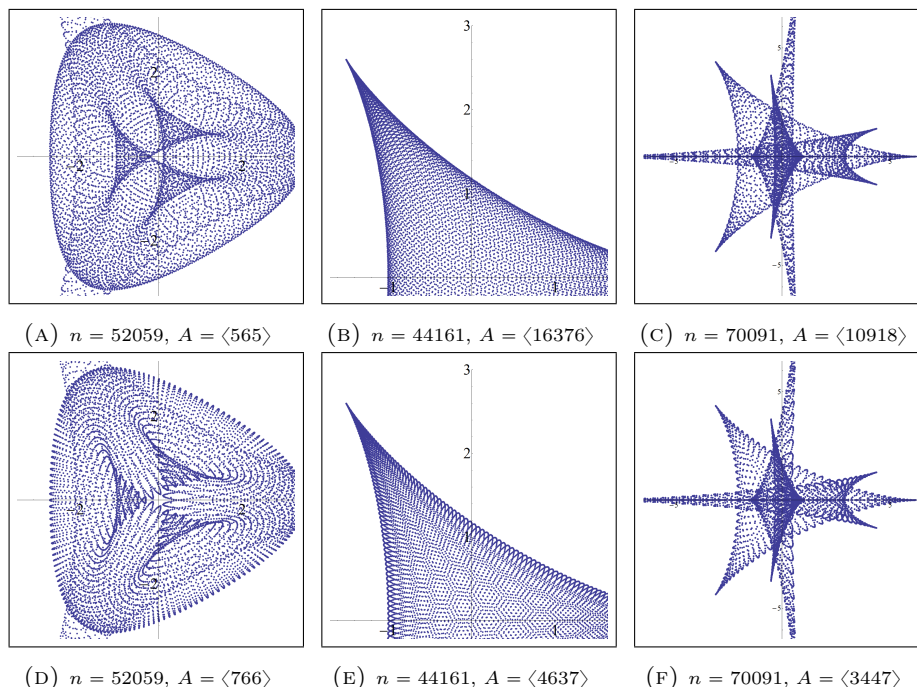


FIGURE 10. Some supercharacters have counterparts whose graphs appear to be geometrically similar while featuring less distinct, “looped” boundaries. Each subfigure is a partial graph of  $\sigma_X$ , where  $X$  is the orbit of  $r = 1$  under the action of  $A$  on  $\mathbb{Z}/n\mathbb{Z}$ .

**Question 5.3.** Most of the techniques developed above depend on the automorphism group  $A$  having a single generator. Can they be extended to apply to automorphism groups having a generating set of any finite order? More generally, what is the graphic nature of supercharacters of  $\mathbb{Z}/n\mathbb{Z}$  arising from non-cyclic automorphism groups?

## REFERENCES

- [1] Berndt, B. C., Evans, R. J., Williams, K. S., *Gauss and Jacobi Sums*, Wiley-Interscience, 1998.
- [2] Diaconis, P., Isaacs, I. M., “Supercharacters and superclasses for algebra groups,” *Trans. Amer. Math. Soc.*, 360(5):2359-2392.
- [3] Isaacs, I. M., *Character Theory of Finite Groups*, AMS, 2006.
- [4] James, G., Liebeck, M., *Representations and Characters of Groups*, Cambridge University Press, 2001.

DEPARTMENT OF MATHEMATICS, POMONA COLLEGE, CLAREMONT, CALIFORNIA, 91711, USA

E-mail address: [Stephan.Garcia@pomona.edu](mailto:Stephan.Garcia@pomona.edu)

URL: <http://pages.pomona.edu/~sg064747>

E-mail address: [Robert.Lutz@pomona.edu](mailto:Robert.Lutz@pomona.edu)